

### **REMARKS**

Claims 1-27 are pending in this application. The Office Action mailed September 27, 2005 rejected claims 1-20, and 22-27. Claim 21 is objected to in the Office Action. Claims 1, 4, 8, 15-16, and 21-22 have been amended in the present response. No new matter has been added. For the reasons discussed in detail below, Applicants submit that the pending claims are patentable over the references cited by the Examiner. Applicants respectfully request that the Examiner pass this application to issue.

#### **Allowable Subject Matter**

The Office Action objected to claim 21 as being dependent upon a rejected base claim, but noted that it would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. In response, Applicants have amended claim 21 to be an independent claim based on the Office Action's recommendation. Therefore, Applicants respectfully submit that claim 21 is now ready for allowance.

#### **Rejection of Claims Under 35 U.S.C. § 102**

The Office Action has rejected claims 1-20, and 22-27 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2002/0087883 to Wohlgemuth et al. (hereinafter "Wohlgemuth"). Applicants respectfully traverse this rejection.

The Applicants respectfully submit that the cited reference does not teach or suggest all of the claim limitations. In particular, the cited reference neither employs the Applicants' detectors, nor does it disclose or suggest sending such detectors to a client process as recited in amended claim 1, nor does it disclose receiving responses at a server for detection by the server. For example, amended Claim 1 recites a method of protecting machine readable media from unauthorized storage or copying by, among other things, "sending a detector to a client process; receiving, at a server, a response to the detector from the client process; and detecting, by the server, a presence of an unauthorized software behavior...."

It is important to note, the Applicants' specification describes the detector as including "a sequence of file system calls generated by an executing program, which can be either exactly or partially matched by a currently executing program's audited file system calls." Such detectors may include a variety of system calls, such as close, open, lock, writes, seek, iocontrol, or the like. (See Applicants' specification, pg. 9, ln. 30 - pg. 10, ln. 2; and Figure 4). Furthermore, one embodiment of the detector may be described as a form of a question. (See Applicants' specification, pg. 8, lns. 27-29). The Applicants' detector may also include more than file system calls, however. (See Applicants' specification, pg. 14, lns. 18-26, and Figure 7 for another embodiment of the Applicants' detector).

Wohlgemuth describes an anti-piracy system for remotely served computer applications that provides a client network filesystem that performs several techniques to prevent piracy of application programs. (See Wohlgemuth, Abstract). However, Wohlgemuth's system is client based and does not rely on the application server to detect and deter piracy attempts. (See Wohlgemuth, par. 0016). In fact, Wohlgemuth's invention is designed around a filesystem at the client side, not the server side. (See Wohlgemuth, par. 0766). Thus, the evaluations and denial of requests pass through the local (client side) network filesystem. (See Wohlgemuth, par. 0766, and 0769). Thus, Wohlgemuth does not disclose or even suggest sending of detectors to the client process, or receiving responses at the server based on the detectors, or detecting a presence of unauthorized behavior by the server, as recited in claim 1.

Wohlgemuth incorporates a number of software anti-piracy techniques. However, none of Wohlgemuth's techniques disclose or suggest the Applicants' rich and complex type of detectors. For example, one of Wohlgemuth's techniques includes "filtering of file accesses based on the surmised purpose of the file access, as determined by examining a history of previous file accesses by the same process." (See Wohlgemuth, par. 0083). In particular, Wohlgemuth's filtering examines entries in a history 4505, 4506 that refer to the file currently being requested. It then runs a heuristic algorithm that tries to determine if the pattern of accesses more closely resembles an attempted file copy than code execution. (See Wohlgemuth, par. 0797). However, the only algorithm that Wohlgemuth discloses is to "simply see if the past n read requests to this file have

been sequential, where  $n$  is some constant. If so, then the request is denied. If not, then the request is granted.” (See Wohlgemuth, par. 0797). Nowhere does Wohlgemuth disclose or suggest the complex type of detectors as claimed by the Applicants. Nowhere does Wohlgemuth disclose or suggest sending such detectors to the client, receiving a response at a server based on the detectors, or detecting by the server a presence of an unauthorized software behavior as is claimed by claim 1.

Moreover, amended claim 1 further includes “updating a database of detectors for a previously unseen and unauthorized behavior of the process, based in part on the response.” Because Wohlgemuth does not disclose nor suggest the use of the Applicants’ detectors, Wohlgemuth does not disclose or suggest updating a database of such detectors. Wohlgemuth does mention using a licensing server; however, nowhere does Wohlgemuth disclose or suggest that the licensing server includes a database of detectors that are updated based on a previously unseen and unauthorized behavior. Thus, for at least these reasons, Wohlgemuth does not anticipate nor make obvious at least claim 1 of the Applicants.

Applicants’ dependent claim 4 recites sending detectors with varying sequence lengths of computer system calls within the detector. Because Wohlgemuth does not disclose the detectors as claimed by the Applicants, Wohlgemuth can not disclose or suggest varying their lengths. As noted above, Wohlgemuth only discloses seeing “if the past  $n$  read requests to this file have been sequential, where  $n$  is some constant.” (See Wohlgemuth, par. 0797). Thus, Wohlgemuth does not disclose varying sequence lengths of the Applicants’ complex detectors as claimed by dependent claim 4. Thus, for at least this reason, the rejection for dependent claim 4 is inappropriate and should be withdrawn.

Similarly, referring to dependent claim 5, because Wohlgemuth does not send detectors as claimed by claim 1, Wohlgemuth can not and does not disclose or suggest encoding numerically the Applicants’ detector such that the meaning of the detector is obscured.

The Applicants’ specification describes three varieties of detectors. For example, one such detector, a novel detector, includes a system call sequence that is a possible behavioral

anomaly, but has not previously been seen. It is employed to recognize new unauthorized software alternations. (See Applicants' specification, pg. 11, lns. 3-22). Applicants' dependent claim 7 claims sending the detector to detect previously unseen and unauthorized behavior to another client process. Because Wohlgemuth does not employ the Applicants' detectors, Wohlgemuth does disclose or suggest sending detectors that detect previously unseen and unauthorized behavior. Thus, for at least these reasons, Wohlgemuth does not anticipate nor make obvious claim 7.

Dependent Claim 8 recites, among other things, exchanging a set of memory detectors between the server and another server, discarding memory detectors...that match another detector in each server's self database, and merging each new retained memory detector within each server's memory database of detectors. Nowhere does Wohlgemuth disclose the limitations of claim 8.

The office action attempts argue that the use of a licensing/licensing server as disclosed in Wohlgemuth teaches such claimed limitation of claim 8. However, the Applicants' disagree. Wohlgemuth merely discloses using such servers to deliver applications to end-user client systems. (See Wohlgemuth, par. 0077-0078). Because, Wohlgemuth does not use detectors as claimed by the Applicants, and Wohlgemuth does not send detectors to the client, nor receive responses back to a server based on the detectors, Wohlgemuth does not disclose exchanging detectors, let alone memory detectors, among the server and another server. As disclosed, Wohlgemuth's licensing servers do not manage databases of memory detectors, as claimed in claim 8. Wohlgemuth simply does not describe sharing of such knowledge of memory detectors between servers to increase their ability to obstruct the spread of unauthorized copying and corruption of electronic media. Thus, for at least this reason, Applicants' claim 8 is neither anticipated nor rendered obvious by the cited reference.

Similarly, independent claim 9 recites, among other things, a method of obstructing unauthorized copying by exchanging a set of memory detectors between servers, evaluating each received set of memory detectors against each server's self database and a set of matching rules, discarding each detector that match another detector in each server's self database, and merging a new retained detector with each server's memory database. Thus, for at least the same reasons as

discussed above for dependent claim 8, Wohlgemuth neither anticipates nor renders obvious independent claim 9. Therefore, the rejection of claim 9 should also be withdrawn.

Amended independent claim 15 recites a method of providing detection of machine-readable media by, among other things, sending by a server, a series of behavioral questions, receiving at the server a response from the client, detecting an unauthorized behavior, and communicating the detection of the unauthorized behavior of the process among a plurality of other servers so that the plurality of other servers are enabled to update their series of behavioral questions based in part on the detected unauthorized behavior. Wohlgemuth does not send a series of behavioral questions by a server to the client, nor receive responses back at the server. Moreover, Wohlgemuth does not disclose nor suggest communicating the detection among a plurality of other servers that are enabled to update their series of behavioral questions. Wohlgemuth does not disclose enhancing of the ability to detect unauthorized behavior across a plurality of servers based on detection by one server. Thus, for at least this reason, Wohlgemuth does not anticipate nor render obvious independent claim 15. Therefore, the rejection should be withdrawn.

Amended independent claim 16 describes a server that includes a program that performs actions, including sending a detector to a client, receiving a response from the client, and updating a database of memory detectors for a previously undetected and unauthorized process on the client. As discussed above, Wohlgemuth does not suggest or disclose the Applicants' detectors, sending such detectors to the client from the server, nor updating a database of memory detectors. Therefore, Wohlgemuth can not anticipate nor render obvious independent claim 16, for at least these reasons.

Independent claim 23 includes a machine readable medium that provides instructions which, when executed by at least one processor causes the processor to perform actions similar, albeit it different, to those of claim 16. Because Wohlgemuth does not suggest or disclose the Applicants' detectors, sending such detectors to the client, nor updating a database of memory detectors, Wohlgemuth can not anticipate nor render obvious independent claim 23.

Dependent claim 19, which depends from independent claim 16, recites wherein the updating [the database] further includes eliminating detectors in the database that exceed a predetermined detector life span. Because Wohlgemuth does not disclose or suggest the Applicants' detectors, Wohlgemuth can not eliminate a detector that exceeds a predetermined life span. Thus, for at least this reason, rejection of claim 19 should be withdrawn.

Amended independent claim 22 recites a computer readable medium having stored thereon a data structure that provides a detector pattern. The data structure includes a plurality of data fields associated with a matching rule; at least one data field indicating a media associated with the detector pattern and each of the remaining data fields comprising a computer system call. As such, claim 22 recites a possible structure of the Applicants' detectors. Because Wohlgemuth does not disclose or suggest such detectors, Wohlgemuth can not anticipate nor render obvious a computer readable medium having stored thereon such a data structure. Therefore, for at least this reason, the rejection of independent claim 22 is inappropriate and should also be withdrawn.

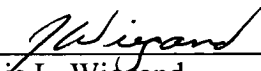
In addition, in regard to claims 2-8, 10-14, 17-20, and 24-27 which are dependent on amended independent Claims 1, 9, 16, and 23 respectively, they are allowable for at least the same reasons discussed above for those independent claims.

**CONCLUSION**

By the foregoing explanations, Applicants believe that this response has responded fully to all of the concerns expressed in the Office Action, and believes that it has placed each of the pending claims in condition for immediate allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue. Should any further aspects of the application remain unresolved, the Examiner is invited to telephone applicant's attorney at the number listed below.

Dated: December 27, 2005

Respectfully submitted,

By   
Jamie L. Wiegand  
Registration No.: 52,361  
DARBY & DARBY P.C.  
P.O. Box 5257  
New York, New York 10150-5257  
(206) 262-8900  
(212) 527-7701 (Fax)  
Attorneys/Agents For Applicant